

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 074-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503				
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE July 1997	3. REPORT TYPE AND DATES COVERED Newsletter Vol. 1 No. 2		
4. TITLE AND SUBTITLE Information Assurance Technology Newsletter		5. FUNDING NUMBERS		
6. AUTHOR(S) Information Assurance Technology Analysis Center				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) IATAC Information Assurance Technology Analysis Center 3190 Fairview Park Drive Falls Church VA 22042		8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Technical Information Center DTIC-IA 8725 John J. Kingman Rd, Suite 944 Ft. Belvoir, VA 22060		10. SPONSORING / MONITORING AGENCY REPORT NUMBER		
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (Maximum 200 Words) This second issue of the Information Assurance Technology Newsletter focuses on the evolution of concepts and definitions pertinent to information assurance. The newsletter also features an overview of the central role that the Defense Intelligence Agency and the Defense Information Systems Agency play in important information operations issues. Featured in this issue: DIA Support to Information Operations Information Assurance Evolves from Definitional Debate				
14. SUBJECT TERMS Information Security, Information Assurance, Information Operations			15. NUMBER OF PAGES 6	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT None	

DTIC QUALITY INSPECTED 4

20001027 072



Information Assurance Technology NEWSletter



IATAC is a Department of Defense Sponsored Information Analysis Center.

Vol. I, No. 2 • July 1997

DIA SUPPORT TO INFORMATION OPERATIONS

The Defense Intelligence Agency (DIA) has demonstrated its commitment to information warfare by establishing the DIA Information Warfare Support Office. Its mission is:

- To produce integrated all-source intelligence supporting U.S. offensive and defensive Information Operations (IO) plans and operations;
- Identify and analyze the IO threat potential and capabilities of foreign nations, transnational groups, or coalitions; and
- Develop detailed intelligence analysis of:
 - Foreign leadership operations and decisionmaking processes;
 - Information technologies, systems, and networks; and

- Denial and deception programs.

The Information Warfare Support Office is made up of four divisions: **Special Activities, Intelligence Preparation of the Battlespace, Threat Analysis, and Foreign Denial and Deception.**

The **Special Activities Division** serves four principal customers: the Unified Commands, the Services, the Joint Staff, and the intelligence community. For the Unified Commands, the division provides intelligence support to OPLAN/CONPLAN information warfare annex development and provides tailored support to Special Technical Operations planning.

The Special Activities Division also

supports the research, development, test and evaluation process of the Services and satisfies information warfare intelligence requirements for the Services.

For the Joint Staff, the division provides political-military assessments; intelligence for contingencies, operations, and deliberate and crisis planning; and tailored, coordinated databases.

For the intelligence community, the Special Activities Division coordinates all-source intelligence for the Special Technical Operations program, interfaces with the collection community, and supports specialized battle damage assessments.

The **Intelligence Preparation of the Battlespace (IPB)** Division provides detailed, all-source, fused intelligence assessments of the operations and decisionmaking processes of the

Continued on page 3



1st Annual Information Assurance Red Team Assessment Workshop Williamsburg, VA on August 13 - 14, 1997

The Defense Information Systems Agency and the Joint Staff (J6K) announce the 1st Annual Information Assurance (IA) Red Team Assessment Workshop to be held August 13 - 14, 1997, at the Fort Magruder Inn (classified sessions at Fort Eustis), Williamsburg, Virginia, under the auspices and sponsorship of the Defense Information Systems Agency and the Joint Staff (J6K) Information Assurance Division.

The workshop is classified **SECRET/US GOVERNMENT ONLY** and provides an opportunity for participants in IA Red Team Assessments to provide input from their research and experiences and

identify what they can provide to mitigate the IA threat.

This Workshop is intended to provide a forum for the discussion, interchange, and debate of accomplishments, discoveries, and issues in the IA area. It is significant because of recent progress made in critical technologies and in the military utilization of these technologies. The Workshop will provide a setting for discussion of the implications of this technology on U.S. government information resources.

To ensure a balanced program for an integrated red team assessment process, the Workshop will consider the various needs of all known customers

as well as the capabilities of current and projected models and simulations and analytical methodologies.

For registration information on the Information Assurance Red Team Assessment Workshop, access the IATAC home page at <http://www.iatac.dtic.mil> on the internet, <http://204.36.65.5/index.html> on Intelink-S, and <http://www.rl.gov/rl/irido/iatac> on Intelink or call Alethia Tucker at (703) 902-4664.

contents

IA Definitional Debate	2
Conferences and Symposia	5
Contacting Us.....	5

Information Assurance Evolves From Definitional Debate

by Dr. John I. Alger
IATAC Director

When the din of battle subsides, observers, pundits, and especially soldiers focus their attention on lessons learned. The 1991 conflagration in Southwest Asia was no exception in this regard, and the examination of the extremely favorable results achieved by the United States and its United Nations allies brought a new level of intensity to the debate concerning the nature of future war.

To some, a new age beckoned; to others, attention to long established tenets of war, such as "mass," "security," and "surprise," proved their worth. Yet even the iconoclasts recognized that "information" had emerged as the prime, if not decisive, contributor to the allied success. The significance of "information" was derived from the phenomenal advances in the realm of digital technology.

Policy and doctrinal guidance have attempted to keep pace with the spiral of information technology advances, but agreement on even the most fundamental definitions has provided a challenge within the Department of Defense (DoD). This article traces the evolution of that definitional debate through the five-plus years since the end of the Gulf War, calls attention to the role of information in the deterrence and prosecution of future war, and hopefully promotes a better understanding of the evolving definitions themselves.

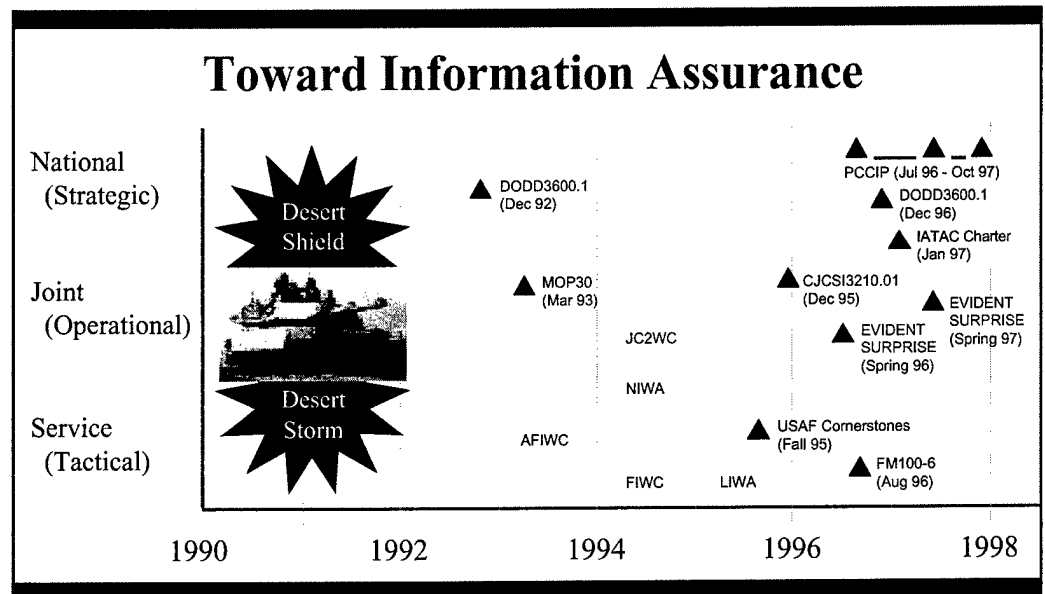
The recognition of the elevated role of information in deterrence and in war was manifested in a revision of the Department of Defense Directive 3600.1, which appeared under the title, *Information Warfare*, in December 1992.

Following the DoD lead on information war, the Office of the Joint Chiefs of

Staff undertook the writing of a complementary publication on new concepts of war demonstrated in the Gulf. The result of the Joint Staff effort was the publication of "Chairman of the Joint Chiefs of Staff Memorandum of Policy Number 30" (MOP 30), in March 1993. It took the title, *Command and Control Warfare*.

these elements did not, however, address the role of computers and networks in future warfare.

To better address the role of information and information systems in future war, the US Air Force transitioned its Electronic Warfare Center at Kelly AFB, San Antonio, TX, to an organization with



MOP 30 defined the relationship between "command and control warfare (C²W)" and "information warfare (IW)" by stating explicitly: "C²W is the military strategy that implements Information Warfare on the battlefield and integrates physical destruction." Implicit in this definition is the recognition that information warfare also occurs "off the battlefield" and that it can be void of "physical destruction."

In addition to defining the relationship between C²W and IW, MOP 30 also stated that C²W encompassed the "integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW) and physical destruction, mutually supported by intelligence."

Widely known as the five pillars of C²W,

a much broader perspective. The new center is called the Air Force Information Warfare Center, and focuses on both the role of information in future war and the need for information assurance. One year later, under the auspices of the Chairman of the Joint Chiefs of Staff, the Joint Electronic Warfare Center, also at Kelly AFB, became the Joint Command and Control Warfare Center. Its focus is on information support to the Commanders-in-Chief of the Unified Commands. Further attention to the primacy of information in future war was evidenced at the National Defense University where the School of Information Warfare and Strategy opened its doors to the first of two 10-month pilot programs in information warfare in August 1994.

Following the lead of the Air Force

Continued on page 3

and the Joint Staff, the Navy and the Army were quick to establish organizations to support the new concepts of deterrence and warfighting. The Navy established the Naval Information Warfare Activity at Fort Meade, MD, and the Fleet Information Warfare Center at Norfolk, VA, with detachments at San Diego, CA, Honolulu, HI, and Chesapeake, VA. The Land Information Warfare Activity was established by the Army at Fort Belvoir, VA. Information assurance is a critical element in each of these organizations.

As each organization pursued concepts and definitions suited to its mission, each was also involved in the definitional debate within the Department of Defense. By 1994, it was widely recognized that the concepts of information warfare were not well served by the definition of information warfare that

appeared in the December 1992 DoD directive. Not surprisingly, each of the principal organizations involved in the concepts of information warfare tailored definitions consistent with and appropriate to its own culture, missions, and doctrine.

Insights into the concepts of each of the major organizations involved in information warfare are clearly seen in the publications of those organizations. The first major organization to promote widely the concept of information warfare was the US Air Force. In the fall of 1995, General Fogleman, the Air Force Chief of Staff, and Secretary Widnall, Secretary of the Air Force, signed the Foreword to a pamphlet entitled, *Cornerstones of Information Warfare*. The pamphlet defined information warfare as: "any action to deny, exploit, corrupt, or destroy the enemy's

information and its function; protecting ourselves against those actions; and exploiting our own military information functions." The pamphlet also detailed six elements of information war. Four were fully consistent with the elements of command and control warfare presented in MOP 30. These were: psychological operations, military deception, physical destruction, and electronic warfare. Where MOP 30 had focused on OPSEC as an element, *Cornerstones* focused on "security measures," which was defined as OPSEC, COMSEC (communications security), and COMPUSEC (computer security). The sixth element of information warfare from the Air Force perspective was "information attack," which was defined as "directly corrupting information without visibly changing the physical

Continued on page 4

DIA SUPPORT TO INFORMATION OPERATIONS

Continued from page 1

national leadership in potential adversary countries to support information operations planning and operations.

The division also develops methodologies for assessing the influence of cultural, psychological, and other human factors on leadership operations and decisionmaking. To support IO targeting, the division produces detailed communications and information system templates of potential adversary countries. Finally, the division provides consultative support to IO operational planners and creates new products and display formats for providing the most useful access to required intelligence.

The **Threat Analysis Division** detects, identifies and assesses IO capabilities of nations, groups, coalitions, and individuals that threaten the U.S. defense and national information infrastructures. Through all-source intelligence products, the division assists in force protection and defensive IO operations. The division also

supports the design and implementation of a defense intelligence warning system for IO attacks, and supports Department of Defense Information Assurance activities.

The Threat Analysis Division also supports the Defense Information Infrastructure, or DII, by producing:

- IO national intelligence estimates,
- System threat assessment reports,
- Country-specific IO threat assessments,
- Information on foreign IO technologies and tools,
- An Electronic Warfare Integrated Reprogramming Data Base, and
- Information on threats to components of the DII.

The **Foreign Denial and Deception Division** of the Information Warfare Support Office detects and analyzes foreign denial and deception directed against U.S. intelligence, national security policy and military strategy, and strategic and conventional targeting, weapons acquisition, military operations, IO, and strategic arms control monitor-

ing. The division detects, identifies, characterizes and monitors foreign underground and enigma facilities and produces all-source intelligence products to support U.S. policy, plans, operations, and acquisitions. Other areas of interest to the Foreign Denial and Deception Division include:

- Foreign denial and deception programs,
- Deception technologies and equipment,
- Foreign perception management,
- Military industrial concealment, and
- Underground facilities and enigmas.

In conclusion, DIA products address the full spectrum of information operations activities. DIA provides integration of intelligence and operations for the warfighter, Defense HUMINT Service information warfare support, information systems support, and a robust open source intelligence program. Since the range of potential contingencies in which the United States is likely to become involved covers the spectrum of conflict, IO support will remain a priority DIA mission area well into the future. ♦

Information Assurance Evolves From Definitional Debate

Continued from page 3

entity in which it resides." Thus, the Air Force elevated the elements of command and control warfare to elements of information warfare. The Air Force also added "information attack" to the taxonomy of IW. These Air Force contributions were indicative of the Air Force's focus on technology and its impact on traditional Air Force missions.

Following the publication of the Air Force's *Cornerstones*, the Chairman of the Joint Chiefs of Staff (CJCS) published CJCS Instruction 3210.01, *Joint Information Warfare Policy*. Its IW definition was identical with the then-current definition in the working draft of DoD Directive 3600.1: "Actions taken to achieve information superiority by affecting adversary information, information-based processes, and information systems while defending one's own information, information-based processes, and information systems." The instruction also discussed the elements of information warfare and spoke of them in terms consistent with MOP 30 and *Cornerstones*.

The third major doctrinal publication to appear, while the revision of DoD Directive 3600.1 was in progress, was the Army's Field Manual 100-6, *Information Operations*. The Army recognized "that IW as defined by DoD was more narrowly focused on the impact of information during actual conflict, [and chose] to take a somewhat broader approach to the impact of information on ground operations and adopted the term information operations." The Army took this view to recognize "that information issues permeate the full range of military operations (beyond just the traditional context of warfare) from peace through global war."

The definition of information operations offered by the Army differed significantly from other official definitions. Army IO was defined as, "Continu-

ous military operations within the MIE [military information environment] that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations; IO include interacting with the GIE [global information environment] and exploiting or denying an adversary's information and decision capabilities." The Army accepted the five C²W elements as a part of IO and added that civil and public affairs were also fully integral to Army IO. Again, the Service's culture established the perspective given to the key definitions and taxonomy of information terms.

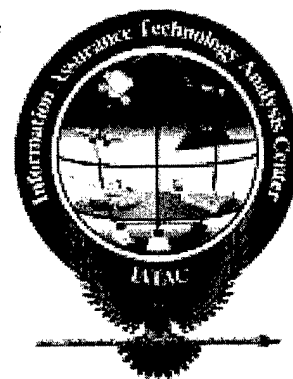
While the publication of key information terms occurred at the Joint Staff level and in the Services, the staffing of the overarching term from a DoD perspective continued for more than two years. The Joint Staff, Air Force, and Army each proposed its own culturally driven terms and definitions. When the new DoD Directive 3600.1 was signed on 9 December 1996, it took the title, *Information Operations*, which hence became the DoD overarching term pertinent to the role of information in warfare. The directive defined Information Operations simply as "Actions taken to affect adversary information and information systems while defending one's own information and information systems." In its discussion of the components of IO, the directive included the elements of C²W from MOP 30, the idea of computer network attack suggested in the Air Force's *Cornerstones*, and the contributions of public affairs and civil affairs as set forth by the Army in FM 100-6. Thus the new DoD Directive had evolved to incorporate the seminal ideas of the Services and other key players in the information arena. It also defined Information Assurance (IA) as: "IO that protect and defend information and information systems. . . ." and stated

that IA activities should be vigorously pursued.

While the key influencing factors in the evolution of the present DoD definition of information operations cited above focused on the Air Force, Joint Staff, and Army, the role of the Navy, Marine Corps, and especially the intelligence community should not be overlooked. The Navy has incorporated the concepts of information operations into their day-to-day fleet activities. The Marines have written about command and control which subsumes information concepts, and similarly the intelligence community has contributed immensely to the process of definition.

From the 1992 DoD Directive on information warfare through each of the publications discussed in this article, the idea of protecting information has been an integral part of every examination of information concepts. The primacy of protecting and defending information has been evident, and today, it is well incorporated into the DoD Directive on Information Operations and in Service publications.

As information operations evolved to accept elements of the earlier definitions of information warfare, so information assurance evolved as the term of choice for defensive IW or command and control protection. The concepts of "protect and defend" are very much in evidence in the DoD Directive 3600.1 definition of information assurance: "Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."



Conferences & Symposia

IIBW9xxx: Intermediate Information Operations/Warfare (IBW)

5 days, Secret Clearance required, O-4 through O-6 and equivalents.
School of Information Warfare and Strategy
National Defense University,
Fort McNair, DC

IBW9801 17-21 Nov 97
IBW9802 12-16 Jan 98
IBW9803 9-13 Mar 98
IBW9804 13-17 Jul 98
IBW9901 19-23 Oct 98
POC: Dr. Fred Giessler,
202-685-2209

SIW9xx: Senior Information Warfare (SIW)

2 days, TS/SCI required, O-7, equivalents and above.
O-6s accepted on waiver
School of Information Warfare and Strategy
National Defense University,
Fort McNair, DC

SIW9801 5-6 Nov 97
SIW9802 12-13 Feb 98
POC: Dr. Fred Giessler,
202-685-2209

Introduction to Information Operations

5 days, TS/SCI Clearance required, O-3 through O-6 and equivalents.
Joint Military Intelligence Training Center, Bolling AFB, DC
20-24 Oct 1997
2-6 Feb 1998
4-8 May 1998
POC: Mr. Doug Dearth, 703-780-2584 – e-mail: dhdearth@aol.com

Information Assurance Red Team Assessment Workshop by DISA and the Joint Staff (J6K)

13-14 August 97
SECRET/US GOVERNMENT ONLY
Fort Magruder Inn, Williamsburg,
VA
POC: 703-902-4664
(See article on page 1.)

infoWARcon '97, "Safeguarding Your Information from Your Competitors" by the National Computer Security Association and Winn Schwartau, Infowar.com

11-12 September 97
Sheraton Premier, Tysons Corner,
VA
POC: 1-800-488-4595, ext 3226

"National Information Systems Security Conference" by the National Computer Security Center at the National Security Agency and the National Institute of Standards and Technology

7-10 October 97 with
Pre-Conference Workshops
on 6 October
Baltimore Convention Center,
Baltimore, MD
POC: 301-975-2775

Information Assurance Technology Newsletter, Vol. 1 No. 2

This second issue of the Information Assurance Technology Newsletter focuses on the evolution of concepts and definitions pertinent to information assurance. The newsletter also features an overview of the central role that the Defense Intelligence Agency and the Defense Information Systems Agency play in important information operations issues.

IATAC, a DoD-Sponsored Information Analysis Center (IAC), is administratively managed by the Defense Technical Information Center (DTIC) under the DoD IAC Program. Inquiries about IATAC capabilities, products, and services, or comments regarding this publication may be addressed to:

Dr. John I. Alger
Director, IATAC
2560 Huntington Avenue
Alexandria, VA 22303-1403



Contacting Us

Telephone: (703) 329-7337
Facsimile: (703) 329-7197
STU-III: (703) 329-3940
STU-III Facsimile: (703) 329-7106
e-mail: iatac@dtic.mil
www: <http://www.iatac.dtic.mil>
Intelink-S: <http://204.36.65.5/index.html>
Intelink: <http://www.rl.gov/rl/irido/iatac>

Distribution & Information

U.S. Distribution Only.

☐ CHANGE ME (as noted below)

☐ ADD ME

☐ SEND IATAC TECHNICAL AREA TASK INFO (Government only)

Name _____

Title _____

Company/Organization _____

Address _____

City/State/Zip _____

Phone _____ Fax _____

DSN _____ E-mail _____

ORGANIZATION: ☐ USA ☐ USN ☐ USAF ☐ USMC ☐ OSD ☐ Contractor

Your Input Is Welcome...

The Information Assurance Technology Newsletter welcomes input from our readers. To submit photographs, related articles, notices, feature programs or ideas for future issues, please use the address, fax or e-mail as noted.



CLIP & SEND TO:
Information Assurance
Technology Analysis Center
2560 Huntington Avenue,
Alexandria, VA 22303-1410

FAX (703) 329-7197

E-mail: iatac@dtic.mil

Information Assurance
Technology newsletter

INFORMATION ASSURANCE TECHNOLOGY



Newsletter



IATAC is a DoD Sponsored
Information Analysis Center

Spring 1998

DEFENDING AGAINST C2W AND IW ATTACK

Editor's Note: This article is part of a continuing series that highlights current Information Assurance (IA) initiatives within the Department of Defense. The Joint Command and Control Warfare Center (JC2WC) is located at Kelly Air Force Base (AFB) in San Antonio, Texas.

*by Colonel Charles C. South, USAF
Deputy Director for Protect/
Defense, Joint Command and
Control Warfare Center*

The mission of the Joint Command and Control Warfare Center (JC2WC) is to "provide direct Command and Control

Warfare support to operational commanders" and serve as the principal field agency within the Department of Defense (DoD) for non-Service-specific C2W support. The JC2WC executes its mission through its directorates of Operations (OP), Protect / Defense (PD), Operations Support and Technical Integration (OT), Systems Integration (SI), the Office of Plans and Programs (XR), and the Special Technical Operations (STO) Division. The focus of the Protect/Defense Directorate is to

assist the combatant commanders in the development of strategies to defend against C2W and Information Warfare (IW) attacks.

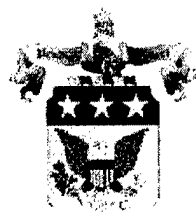
The Directorate's original concept was that of "Red Teaming" or exploiting information operations and related information technologies to raise the awareness of CINCs and OSD program managers to information related vulnerabilities. However, as concepts and doctrine for IW and Information Operations (IO) developed, we realized that

Continued on page 2.

INSIDE

Penetration Testing Course	3
IA Tools Database:	
Intrusion Detection	4
STINET	6
IATAC Products	6
Conferences & Symposia	7
Penetration Testing Course Registration	8

INFORMATION ASSURANCE SEMINAR GAME



The U.S. Army War College, Center for Strategic Leadership, hosted an Information Assurance Seminar Game that examined the emerging roles of the public and private sectors in protecting our critical information infrastructures from Information Warfare attacks. The Seminar Game was held 3-5 February 1998 at the Center for Strategic Leadership (CSL) Carlisle Barracks, Pennsylvania and was jointly sponsored by the CSL, Booz-Allen & Hamilton, and the National Computer Security Association. Seminar Game participants were composed of industry and government experts whose views influence national information assurance policy and direction. The Seminar Game provided participants with a unique opportunity to interact on matters of increasing concern to all, and resulted in a more balanced view of information warfare and its threat to our nation's critical infrastructure, private and public.

Presentations by recognized national security experts were provided to help participants define the threat, assess vulnerabilities and consider ways to estimate damages in the wake of an in-

formation infrastructure attack. Participants investigated ways to detect and disclose infrastructure attacks while addressing an appropriate process for response and recovery. The seminar also considered the national response to a strategic information attack.

Results of the game will be distributed to participants, key government offices, and selected agencies for publication. Further details can be obtained by contacting one of the following:



U.S. Army War College
Mr. Robert F. Minehart, Jr. (717) 245-4472

International Computer Security Association
Mr. Fred Tompkins (717) 241-3241

Booz-Allen & Hamilton, Inc.
Mr. Albert J. Ross (410) 684-6635

The Information Assurance Technology Newsletter is published quarterly by the Information Assurance Technology Analysis Center (IATAC). The third issue continues the focus on current information assurance initiatives underway within the Department of Defense. In addition, an overview of the IA Tools Database is provided that highlights the current collection of Intrusion Detection Tools.

ATAC, a DoD-Sponsored Information Analysis Center (IAC), is administratively managed by the Defense Technical Information Center (DTIC) under the DoD IAC Program. Inquiries about ATAC capabilities, products and services may be addressed to:
Robert Thompson
Assoc. Director, IATAC

We welcome your input. To submit your related articles, photos, notices, feature programs or ideas for future issues, please contact:
IATAC
ATTN: C. Wright
8283 Greensboro Dr.
Allen 663-D
McLean, VA 22102
Phone 703-902-3177
Fax 703-902-3425
STU-III 703-902-5869
STU-III Fax 902-3991
E-mail: iatac@dtic.mil
Internet: www.iatac.dtic.mil
ntelink-S:
http://204.36.65.5/index.html
ntelink:
http://www.web1.rome.c.gov/iatac

IO vulnerabilities should be addressed in the larger context of IW and IO. That is, since command and control (C2) is a subset of IW, we need to protect information with C2 application and value, regardless of whether or not it resides in a C2 system. In addition, we need to address those IO objectives and tasks associated with peacetime defense.

Accordingly, the Protect/Defense Directorate's mission is evolving from (C2) Protect and (IW) Defense to Defensive IO. In this context, we are orienting our mission to the new definitions prescribed by DODD S-3600. (*Information Operations*), CJCSI 3210.1 (*Joint Information War - Fare Policy*), CJCSI 651001A (*Defensive IW Implementation*), and Draft Joint Pub 3-13 (*Joint Doctrine for Information*

Operations). DODD S-3600 provides that "DoD information systems critical to the transmission and use of minimum-essential information for command and control of forces shall be designed, employed, and exercised in a manner that minimizes or prevents exploitation, degradation, or denial of service from a multiple variety of attacks to include computer network attack." Draft Joint Pub 3-13 refers to the following related defensive IO areas: information assurance, physical security, OPSEC, counter-deception, counter-PSYOP, counter intelligence (CI), electronic protect, and special information operations. The Defense IO mission also involves responses to IW attacks that may be either defensive or offensive in na-

ture and may involve interface with law enforcement agencies.

As you can see, Defensive IO is a relatively broad mission. It is also a dynamic one — as IW and IO concepts and doctrine evolve, so does our mission, and we continue to examine processes that best support the combatant commanders in the areas listed above. Since this is a new mission area for the JC2WC, we continue to seek out the best training available in these areas to enable us to provide the requisite expertise as a "center of excellence." To accomplish this mission, the Directorate has established three functional area teams (see Figure 1 below) to respond to our evolving defensive IO mission. These

Continued on page 7.



Figure 1. Protect/Defense Functional Areas

PENETRATION TESTING COURSE

Course Objective:

The purpose of this full-day tutorial is provide attendees an accurate depiction of the role penetration testing plays in analyzing a system's overall security posture. The tutorial is designed to provide a thorough understanding of penetration testing concepts, terminology, approaches and techniques that can be applied to all system and network configurations.

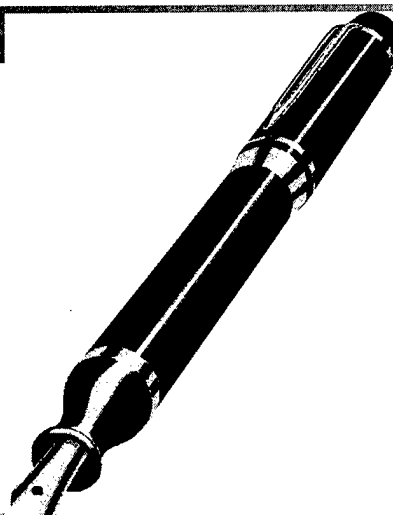
This course is NOT intended to teach specific system vulnerabilities or how to exploit them, but will provide information on publicly available sources and tools that are commonly used by hackers. During this course attendees will learn how penetration testing fits into life-cycle system/network security and how it can complement other commonly performed security activities such as risk analysis and security test and evaluation. Attendees will also learn the limitations to penetration testing and that it is not a comprehensive analysis of a system's security.


At the completion of this tutorial, attendees should have a better understanding of what penetration testing is and is not, how it can be beneficial to organizations, and restrictions imposed when performed by professional consultants within legal boundaries. Attendees will have obtained the basic foundation necessary for building a penetration testing capability and performing penetration tests.

The tutorial will be held as Government-Only (see registration form on page 8) at the Booz-Allen & Hamilton McLean

Campus — 8283 Greensboro Drive. A registration fee of \$225.00 is required and due by May 18, 1998. A \$50.00 late fee will be applied for all registrations received after May 18, 1998 and for payment at the door.

For more information concerning the tutorial, please contact Christina Wright at 703-902-3176/3177 or via e-mail at iatac@dtic.mil.





Penetration Testing Tutorial

Instructor: Debra Banning

Course Outline:

1. Introduction to Penetration Testing
2. Approaches to Penetration Testing
3. Building a Penetration Testing Capability
4. Penetration Testing Scenarios
5. Performing Penetration Testing

JUNE 4

MCLEAN, VA

**FULL DAY
COURSE**

**REGISTRATION
DEADLINE**

18 MAY 98

**COST
\$225.00**

**GOVERNMENT
ONLY**

ABOUT THE INSTRUCTOR

Debra Banning is a Senior Associate at Booz-Allen & Hamilton specializing in security/risk assessments and penetration testing. Ms. Banning has been planning, performing and leading penetration exercises for government and commercial clients for 13 years. She recently presented the Penetration Tutorial on which this workshop is based at the 13th Annual Computer Security Applications Conference sponsored by the IEEE Computer Society.

INFORMATION ASSURANCE TOOLS DATABASE: INTRUSION

The **IATAC Information Assurance Tools Database** hosts information on intrusion detection, vulnerability analysis, firewalls, and anti-virus applications. A brief summary of Intrusion Detection Tools is provided on these two pages. For more information, see **IATAC Products** on page 6.

Title	Attributes	Description
ADS	attack detection	Attack detection system for secure computer systems
AID	audit-based, misuse detection	Distributed intrusion detection system that consists of agents on the monitored hosts and a central monitoring station with an expert system
ALVA	anomaly detection, audit-based	Real-time tool for detecting potential security violations in UNIX audit logs. The system gains some level of platform independence by analyzing command logs that are pre-computed from the system audit logs.
Argus	audit-based, system monitoring	Generic IP network transaction auditing tool for UNIX
ARPMon	system monitoring	Maps IP addresses to physical network or hardware addresses to monitor the usage of IP addresses on a network
ARPPWATCH	system monitoring	Aims to protect against address spoofing by monitoring Ethernet activity and maintaining a database of Ethernet/IP address pairings
ASAX	audit-based, misuse detection	Distributed audit trail analysis system that also has incorporated configuration analysis
ASIM	anomaly detection	Air Force project designed to measure the level of unauthorized activity against its systems
CMDS	anomaly detection, audit-based, expert system, misuse detection	Real-time audit reduction and analysis to detect and deter computer misuse
Courtney	system monitoring	Monitors the network and identifies the source machines of SATAN probes/attacks
CyberCop	anomaly detection, misuse detection, system monitoring	Real-time security solution that issues alarms when attacks are identified, recognizes networked elements under attack, logs the activity, and captures evidence of the intrusion
EMERALD	anomaly detection, system monitoring	Distributed scalable tool suite for tracking malicious activity through and across large networks and introduces a highly distributed, building-block approach to network surveillance, attack isolation, and automated response
Gabriel	system monitoring	SATAN detector available for Sun platforms, written entirely in C and comes pre-built
GrIDS	anomaly detection	Uses graph-based language for analyzing network connection activity in a LAN-MAN sized system to detect large-scale automated attacks on networked systems
IDES	anomaly detection, expert system, misuse detection, system monitoring	Real-time intrusion-detection expert system that observes user behavior on a monitored computer system and adaptively learns what is normal for individual users, groups, remote hosts, and the overall system behavior
IDIOT	misuse detection	Based on complexity of matching and temporal characteristics
Ifstatus	anomaly detection	Checks network interfaces for promiscuous or debug mode in an attempt to determine if a sniffer is being run
Internet Scanner Toolset	anomaly detection	Perform scheduled and selective probes of a network's communication services, operating systems, key applications, and routers in search of those vulnerabilities most often used by individuals to probe, investigate, and attack
INTOUCH INSA	anomaly detection, keystroke surveillance, misuse detection	Scans all network-based user activity, regardless of the computer manufacturer or operating system being used, utilizing keystroke-level surveillance
ITA	anomaly detection, audit-based, misuse detection	Detect intruders or abuse by analyzing audit data from the operating systems it supports utilizing a rules engine
Kane Security Monitor	misuse detection, system monitoring	Provides network security monitoring using artificial intelligence, and identifies internal and external violations
md5check	file integrity	Compares the MD5 checksums of several critical SunOS 4.x system files to a database
NADIR	anomaly detection	Rules-based expert system to automatically detect intrusion attempts and other network security anomalies

DETECTION TOOLS

Title	Attributes	Description
NETMAN	system monitoring	Package of network monitoring and visualization tools for monitoring and displaying network communications
NetRanger	anomaly detection, misuse detection, system monitoring	Analyzes the data traffic for content and context while searching for signatures indicative of hacking attacks or other security violations
NID	anomaly detection, misuse detection	Detects, analyzes, and gathers evidence of intrusive behavior on Ethernet and FDDI networks using the Internet protocol
NIDES	anomaly detection, expert system, misuse detection, system monitoring	Real-time monitoring of user activity on multiple target systems connected via Ethernet. rule-base employs expert rules to characterize known intrusive activity represented in activity logs, and raises alarms.
NOCOL	system monitoring	Monitors network and system variables, such as ICMP or RPC reachability, RMON variables, nameservers, Ethernet load, port reachability, host performance, SNMPtraps, modem line usage, Appletalk and Novell routes/services, BGP peers
Noshell	system monitoring	Provides the system administrator with additional information about who is logging into disabled accounts
NSM	system monitoring	Network-based network traffic monitor
POLYCENTER	misuse detection, system monitoring	Knowledge-based analysis of audit data to recognize and respond to simple security-relevant events
RealSecure	system monitoring	Real-time, automated attack recognition and response system that rests on the network, monitoring the network traffic stream looking for attacks and unauthorized access attempts
SecureNet Pro	keyword-level surveillance, system monitoring	Combines several key technologies, including session monitoring, firewalling, hijacking, and keyword-based intrusion detection
Stake Out	anomaly detection, misuse detection, system monitoring	Monitors network traffic and detects intrusive or suspicious activity as it occurs
Stalker	misuse detection	Identifies intruders and internal misuse by analyzing audit trail data and reporting on suspicious user and system activities
Swatch	misuse detection, system monitoring	Monitors events on a large number of systems and modifies certain programs to enhance their logging capabilities and software to then monitor the system logs
Tripwire	file integrity	Compares a designated set of files and directories to information stored in a previously generated database
T-sight	system monitoring	Visualizes traffic and data transiting a network, evaluates risks of certain transactions, and displays connection/transaction data that can either be logged or viewed during real-time monitoring
UNICORN	audit-based	Accepts audit logs from Unicos (Cray UNIX), Kerberos, and a common file system, then analyze them and attempts to detect intruders in real time
JSTAT	misuse detection, state transition analysis	Makes use of the audit trails that are collected by the C2 Basic Security Module of SunOS and keeps track of only those critical actions that must occur for the successful completion of the penetration
WatchDog	system monitoring	Monitors and manages the SunOS audit trail produced by the system's C2 security features and responds in real time to events that appear, and stores the audit trail
WebStalker Pro	misuse detection	Controls access to Web content files, and can watch all Web and non-Web accesses, all processes, and all changes to Web and other files; notifies in realtime through SNMP, pager, or e-mail when anything suspicious occurs
X Connection Monitor	system monitoring	Monitors X connections by using RFC931 to display user names, when the client host supports RFC931, and allows the user to freeze and unfreeze connections, or kill them, independent of the client and independent of the server

IATAC PRODUCTS

For more information on IATAC products & reports, contact Alethia Tucker at 703-902-3177.



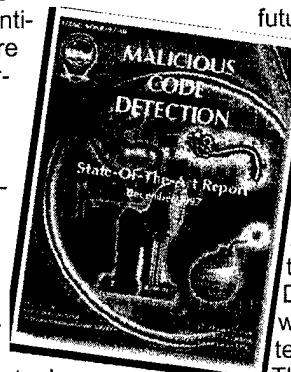
MODELING & SIMULATION TECHNICAL REPORT

This unclassified report describes the models, simulations and tools being used or developed by selected organizations that are chartered with the Information Assurance mission. Data collection efforts focused on the current definitions of Information Operations, Information Warfare, and Information Assurance as described in DoD Directives S-3600.1, "Information Operations," and Chairman, Joint Chiefs of Staff Instruction 6510.1A, "Defensive Information Warfare Policy." In addition, the definitions prescribed by DMSO for model and simulation were used to determine what entities should be included in this IA models, simulations and tools report.



INTRUSION DETECTION TOOLS REPORT

This Information Assurance Tools Report provides an index of intrusion detection tool descriptions contained in the IATAC Information Assurance (IA) Tools Database. The IA Tools Database hosts information on intrusion detection, vulnerability analysis, firewalls, and anti-virus software applications. Information was obtained via open source methods, including direct interface with various agencies, organizations, and vendors. Research for this report identified 43 intrusion detection tools currently employed and available. Tool information includes title, author, source, contact information and tool abstract.



MALICIOUS CODE DETECTION SOAR

This IATAC State-Of-The-Art Report (SOAR) addresses Malicious Software Detection. Included within the report is a taxonomy for malicious software to provide the audience with a better understanding of commercial malicious software. An overview of the current state-of-the-art commercial malicious software detection products and initiatives, as well as future trends is presented. The same is then done for current state-of-the-art in regards to DoD malicious software detection. Lastly, the report presents observations and assertions to support the DoD as it grapples with this problem entering the 21st century. This report is classified and has a limited release.

SECURE STINET'S CUSTOMIZATION



The Dynamic Secure STINET Service now has added the following:

Secure STINET's Customization provides the power to create and modify your own personalized web page. See what has changed in STINET by filtering out what is old and concentrating on what is new...set up a personal profile based on subject fields and groups and automatically receive citations via e-mail to the latest accessions in DTIC's Technical Report collection twice a month...save search queries for both the Technical Report and Work Unit Information System collections for reuse.

Abstracts are now included with citations to unclassified/ limited documents in the Technical Reports Bibliographic Database. Viewing abstracts is based on individual user

profile access restrictions. If your profile does not permit you to view a particular citation's abstract, you will be allowed to view the rest of the citation, minus the abstract.

Over 3,000 full-text technical reports are now available for viewing and downloading. Special Collections highlights reports found in DTIC's Technical Reports collection based on the source, topic, or targeted group. In addition to setting up your own search parameters, you can search using preestablished profiles developed by retrieval experts.

The Partnership for Peace Information Management System (PIMS) is designed to enhance the education of U.S. Service school students. Topic searches developed by DTIC for the PIMS community provide information ranging from air traffic control management to public affairs. PIMS also offers students the capa-

bility to construct custom searches for information not covered in the topic searches.

The subscription for the Secure STINET Service access via a web client is \$50 per year/per subscriber. To subscribe to Secure STINET Service, contact DTIC's Registration Branch:

Telephone: (703) 767-8272
DSN 427-8272

Toll Free: 800-225-3842
(menu selection 2, option 2, sub-option 2)

Fax: (703) 767-8228
DSN 427-8228

E-mail: reghelp@dtic.mil

Questions concerning this product may be directed to the Product Management Branch, DTIC-BCP, 800-225-3842 (menu selection 2, option 3), 703-767-8267, or DSN 427-8267.

DEFENDING....

Continued from page 2.

functional teams are entitled Combat Support, Advanced Technology, and Field Support. Since the directorate is relatively small, with only 17 people, we leverage IO "opposition force" and analytical capabilities of other national agencies, service IW activities, and contractors.

The Protect/Defense Directorate supports six to eight CINC-sponsored exercises each year. The Combat Support Team provides direct defensive IO support to the combatant commander and serves as the joint coordination focal point for vulnerability assessment (i.e., exercise CONOP), IW Red Team scenario development, external agency coordination, defensive IO awareness training (as requested), Red Team scenario execution, and After-Action-Reporting.

The JC2WC has been asked by OSD to perform vulnerability assessments in support of the Advanced Concept Technology Demonstration (ACTD) program. During FY97, the Advanced Technology Team provided vulnerability assessment support for the following ACTDs: Rapid Terrain Visualization, Counter Proliferation, Air Base/Port Bio Detection, Combat ID, Battlefield Awareness and Data Dissemination, Joint Counter-nine, Rapid Force Projection initiative, and Precision SIG-NT Targeting System. ACTDs tentatively planned for evaluation in FY98 include Navigation Warfare, Joint Logistics, Military Ops in Urban Terrain, Extended Littoral Battlespace, Chemical Add-on (to Air Base/Port Bio Detection), and Unattended Ground Sensor. Vulnerability assessment support provides critical insight into system design and allows

OSD and the Services to correct deficiencies before production and fielding of a system. As such, CINC users are made aware of the limitations associated with a system before depending on the information in an operational environment. Other FY98 approved ACTDs are still under review for assessment.

The Field Support Team functions as a self-sustaining, deployable "IW Red Team" that supports the Combat Support and Advanced Technology teams. Field Support Team deployable capabilities include HF/VHF/UHF/ EHF, Signal Intercept and DF, Radar/IR Detection, and RF Jamming. Instrumentation assets include GPS, oscilloscopes, pulse analyzer, and spectrum analyzer. In addition, Field Support Team assets include shelters, generators, and cargo trucks.

As the IO environment becomes more complex, and the Defense Information Infrastructure more integrated with the National and Global Information Infrastructures, defensive IO measures also become more important and more difficult to assure. In any case, we will continue to leverage heavily off of the resources and capabilities of National agencies such as National Security Agency (NSA) and the Services' IW Centers/Activities in providing defensive IO support to the combatant commanders. The JC2WC will continue to strive to be the acknowledged IO leader, responsive to the CINCs, for integrating information operations into the overall military campaign plan.

' CJCSI 5118.01. Charter for the Joint Command and Control Warfare Center, 15 September 1994.

CONFERENCES & SYMPOSIA

Fiesta Informacion '98

Convention Center • San Antonio, TX
"The Virtual Enterprise in the 21st Century"
For information call 800-564-4220
14—16 Apr 98

10th Ann. Software Technology Conference

Salt Palace Convention Ctr, Salt Lake City, UT
"Knowledge-Sharing — Global Information Networks."

<http://www.stc98.org>
19—24 Apr 98

USPACOM Information Assurance Conference

Honolulu, HI
POC: SFC Huff 808-477-1046
e-mail: huffsd00@hq.pacom.mil
28—30 Apr 98

Introduction to Information Operations

TS/SCI clearance, O-3 through O-6 and equivalents, Bolling AFB, DC.
POC: Mr. Doug Dearth
703-780-2584
e-mail: dhdearth@aol.com
4—8 May 98

Penetration Testing Course

This course is Government Only. Booz•Allen & Hamilton McLean Campus. See page 3 for complete description. <http://www.iatac.dtic.mil>
4 Jun 98
Fee: \$225.00
Registration form on back of newsletter.

IIBW9xxx: Intermediate Information Operations/Warfare (IBW)

5 days, SECRET clearance required, O-4 through O-6 and equivalents, School of Information Warfare and Strategy, National Defense University, Fort McNair, DC
POC: Dr. Fred Giessler, 202-685-2209
IBW9804 13—17 Jul 98
IBW9901 12—23 Oct 98

PENETRATION TESTING COURSE REGISTRATION

JUNE 4, McLEAN VA

(Government Only)

Title _____

Attendee Name _____

Organization (Govt. or Military) _____

Organization Address _____

Phone _____ Fax _____

E-mail _____

Fee \$225.00 (Add \$50.00 after 18 May 1998)

☐ Check enclosed for \$ _____

Attach payment and mail by 18 May 98 to:

*IATAC, 8283 Greensboro Drive, Allen 663-D
McLean, VA 22102-3838*

DISTRIBUTION & INFORMATION

U.S. Distribution Only

- ☐ Change ☐ Add
☐ Send IATAC Technical Area Task Info (Govt Only)

Name _____

Title _____

Company/Org. _____

Address _____

City/State/Zip _____

Phone _____

Fax _____

DSN _____

E-mail _____

Organization (check one):

- ☐ USA ☐ USN ☐ USAF ☐ USMC ☐ OSD
☐ Contractor



**Information Assurance
Technology Analysis Center
8283 Greensboro Drive, Allen 663
McLean, VA 22102-3838**

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 074-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503				
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE Fall 1998	3. REPORT TYPE AND DATES COVERED Newsletter Vol. 2 No. 2		
4. TITLE AND SUBTITLE Information Assurance Technology IA Newsletter		5. FUNDING NUMBERS		
6. AUTHOR(S) Information Assurance Technology Analysis Center				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) IATAC Information Assurance Technology Analysis Center 3190 Fairview Park Drive Falls Church VA 22042		8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Technical Information Center DTIC-IA 8725 John J. Kingman Rd, Suite 944 Ft. Belvoir, VA 22060		10. SPONSORING / MONITORING AGENCY REPORT NUMBER		
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (Maximum 200 Words) The IANewsletter is published quarterly by the Information Assurance Technology Analysis Center (IATAC). This issue continues the focus on current information assurance initiatives underway within DoD, academia, and industry. In addition, an overview of the current collection of Firewall Tools is provided. Also, featured in the issue: Protecting Our Critical Infrastructures Through Public-Private Partnership Detecting Intrusions Cooperatively Across Multiple Domains Secure Your Distributed Network: What Will It Take?				
14. SUBJECT TERMS Information Security, Information Assurance, Information Operations, Intrusion Detection			15. NUMBER OF PAGES 16	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT None	



Vol. 2, No. 2
Fall 1998

The Defense-Wide Information Assurance Program

by CAPT J. Katharine Burton, USN
DIAP, OASD (C3I)/IA

The Department of Defense's increasing dependence on a global information environment heightens its exposure and vulnerability to a rapidly growing number of sophisticated internal and external threats. Globally inter-networked and interdependent information systems tend to level the playing field between allies and potential adversaries. These systems offer adversaries access to potentially low-risk, high-value information infrastructure targets with the potential to impact the full spectrum of DoD operations. Furthermore, with each advance in information technology, new vulnerabilities are created that must be quickly discovered and effectively neutralized.

Before global networking became commonplace, the majority of the Department's critical information functions, both command & control and support, were electrically separated in Component-managed telecommunications and information processing environments. This separate-system condition had the advantage of providing the Department's information and information systems a level of resiliency and protection, forcing an adversary to attack each independently controlled environment. To seriously degrade the aggregate capability of the Department, an adversary must disrupt or corrupt a large number of critical systems using highly sophisticated (and largely unavailable) technologies that were expensive

in terms of both time and money.

In contrast, the Department's reliance on commercial, globally interconnected information technologies has markedly heightened its vulnerability to attack. Today's inter-networked information technologies make it possible to affect many users, systems, and networks by attacking a single connection to a single network. To attack a large number of systems, an adversary need only find and attack a single exploitable connection to the system. These attacks can be performed through the use of a large and growing variety of available and inexpensive hacker tools. Once inside a system, an adversary can exploit it, as well as the systems networked to it. This glob-

continued on page 2

IATAC

is a DoD-Sponsored
Information Analysis
Center Administered by the
Defense Technical
Information Center (DTIC).



INSIDE

3 Protecting Our
Critical Infrastructures Through Public-Private Partnership

6 R&DPerspective:
Intrusion Detection
System Evaluation

8 IA Tools Summary:
Firewalls

10 Detecting Intrusions
Cooperatively Across
Multiple Domains

11 Secure Your Distributed Network:
What Will It Take?

12 IATAC chat

13 Calendar

14 What's New

15 IATAC Product
Order Form



Internet Presents



year, Air Force Lt. Col. Buzz Walsh and Maj. Brad Ashley presented a series of briefings to top DoD leaders that raised more than just a few eyebrows.

Selected leaders were shown how it was possible to obtain their individual social security numbers, unlisted home phone numbers, and a host of other personal information about themselves

families—sim-
cruising the
it.

and Ashley, members of the Pentagon's staff, were not just a joke on leaders. Nor were they trying to



be clever. Rather they were dramatically, and effectively demonstrating the ease of accessing and gathering personal and military data on the information highway — information which, in the wrong hands, could translate into a vulnerability.

"You don't need a Ph.D. to do this," Walsh said about the ability to gather the information. "There's no

by Paul Stone
American Forces Information Service

rocket science in this capability. What's amazing is the ease and speed and the minimal know-how needed. The tools (of the Net) are designed for you to do this."

The concern over personal information on key DoD leaders began with a simple inquiry from one particular flag officer who said he was receiving a large number of unsolicited calls at home. In addition to having the general's unlisted number, the callers knew specifically who he was.

Too Much About Too Much

Beginning with that one inquiry, the Joint Staff set out to discover just how easy it is to collect data not only on military person-

continued on page 4

Vol. 2 No. 2

The IANewsletter is published quarterly by the Information Assurance Technology Analysis Center (IATAC). This issue continues the focus on current information assurance initiatives underway within DoD, academia, and industry. In addition, an overview of the current collection of Firewall Tools is provided.

IATAC, a DoD-Sponsored Information Analysis Center (IAC), is administratively managed by the Defense Technical Information Center (DTIC) under the DoD IAC Program. Inquiries about IATAC capabilities, products and services may be addressed to:

Robert Thompson
Director, IATAC
703.902.5530

We welcome your input!

To submit your related articles, photos, notices, feature programs or ideas for future issues, please contact:

IATAC
ATTN: C. McNemar
8283 Greensboro Dr.
McLean, VA 22102
Phone 703.902.3177
Fax 703.902.3425
STU-III 703.902.5869
STU-III Fax 902.3991

E-mail: iatac@dtic.mil
URL: www.iatac.dtic.mil

Art & Production Director
C. McNemar
Information Processing
Robert Weinhold
Information Collection
Alethia A. Tucker
Inquiry Services
Peggy O'Connor
Contributing Editor
Martha Elim

al marriage of systems and networks has created a *shared risk environment*.

Any risk of weakness in any portion of the Defense Information Infrastructure (DII) is a serious threat to the operational readiness of all Components. The Department is moving aggressively to ensure the continuous availability, integrity, authentication, confidentiality, and non-repudiation of its information, and the protection of its infrastructure. Recent assessments, exercises, and real-life events clearly demonstrate that Defense-wide improvements in Information Assurance (IA) are an absolute and continuous operational necessity. We can no longer be satisfied with reactive or after-the-fact solutions. As the Department modernizes its information infrastructure, it must continuously invest in the research, development, and timely integration of products, procedures, and training necessary to sustain its ability to defend and protect the infrastructure. Providing for the protection of the DII is among the Department's highest priorities and is one of its most formidable challenges.

The Department's IA objective is to provide for the availability, integrity, authentication, confidentiality, non-repudiation, and rapid restoration of DII mission essential elements. Critical to achieving this objective is the implementation of a Department-wide planning and integration framework. To that end, on January 30 the Deputy Secretary of Defense, Dr. John J. Hamre, approved the creation of the Defense-wide Information Assurance Program (DIAP). The recommendations of the program are the result of several years of effort by the IA community, including:

- The October 9, 1996, Program Decision Memorandum II (PDM II) directing that an assessment be conducted by the Department-wide Information Assurance Task Force, and
- The August-September 1997 IA Integrated Process Team (IA

IPT) effort directed by a Secretary of Defense memorandum of August 12, 1997.

The recommendations reflect the Department's understanding that IA is an operational readiness issue and that its dependence on inter-networked systems and services creates a shared risk environment necessitating an unprecedented level of coordination and unity across the Department. The DIAP will provide the common management framework and central oversight necessary to ensure the protection and reliability of the DII. While planning and integration will be centralized, execution of individual Components' programs will remain the responsibility of the Components. A culture that recognizes and values IA must also be built among all Department Components.

Accordingly, the DIAP will continuously compare Department's IA programs and functions against its operational and business information requirements, Defense-wide readiness standards, and threats to the DII. The DIAP will also infuse IA throughout its operations as a fundamental element of readiness and training. Operational readiness standards will be used to assess the adequacy of the protection afforded to the Department's data, information systems, and networks, and to the entire DII. This effort will provide a comprehensive and

real-time picture of all IA programs. It will enable the Department to accurately develop, validate, and prioritize IA requirements; determine the return on its IA investments; and objectively assess its protection efforts.

The DIAP achieved initial operational capability in June 1998 with

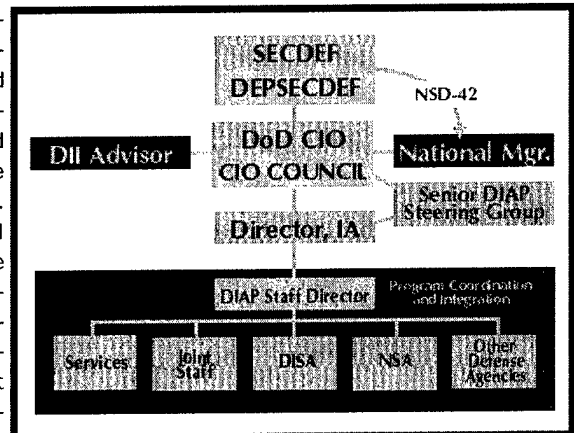


Figure 1.

the assignment of the Staff Director and other key positions. It is in the process of achieving full operational capability as staffing for the various positions becomes available. Organizationally, the DIAP reports to the Information Assurance

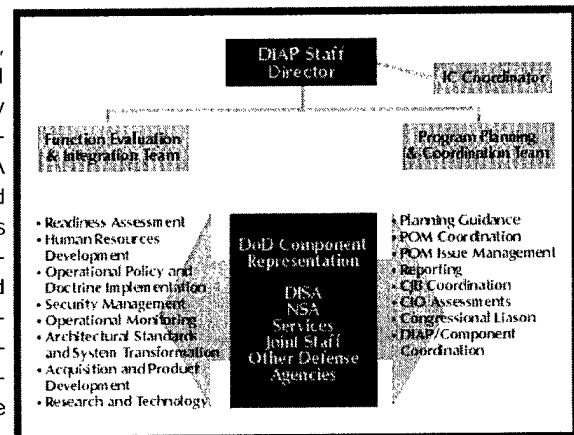


Figure 2.

Directorate of the Office of the Assistant Secretary of Defense for C3I (OASD/C3I) (Figure 1). The DIAP is divided into two teams: the Functional Evaluation and Integration Team (FEIT) and the Program Development and Integration Team (PDIT) (see Figure 2). Between

Protecting Our Critical Infrastructures Through Public-Private Partnership

by Kenneth M. Geide, National
Infrastructure Protection Center, FBI

As our society speeds into the Information Age, we are growing increasingly dependent on a complex web of information systems to manage our lives. We use computers, the Internet, and other information technologies to conduct business, manage finances, engage in personal communications, and process vast amounts of data.

This dependence on information systems also extends to our Nation's critical infrastructures. These infrastructures (telecommunications, energy, banking and finance, transportation, and government operations, among others) are the foundation of our economy, national security, and way of life; virtually every citizen depends on them everyday. Technological advances have made these infrastructures highly automated and interdependent, increasing their efficiency and improving the quality of their services.

Yet technological advances have also introduced vulnerabilities into these infrastructures, and more people now have the tools to exploit them. For example, the pervasiveness and easy accessibility of the Internet means that anyone possessing the right tools and technical skills can penetrate an organization's information and control systems to steal data or inflict damage. Culprits who might commit such acts include disgruntled employees, recreational hackers, criminal groups, terrorist organizations, foreign intelligence services, or even hostile nations.

The National Infrastructure Protection Center (NIPC) was established in February 1998 to address infrastructure threats and vulnerabilities. Our mission is to detect, deter, assess, warn of, respond to, and investigate unlawful acts (both physical and cyber) that threaten

our critical infrastructures. Located at FBI Headquarters in Washington, D.C., the NIPC is an interagency, public-private body that brings together investigators, analysts, computer scientists, and other experts from government and private industry.

The NIPC focuses on preventing attacks (learning about them before they occur) and taking steps to prevent or disrupt them. This effort requires collecting and analyzing information from all available sources (including law enforcement, intelligence services, open sources, and the private sector) and disseminating our analyses to all relevant organizations. If an attack occurs, the NIPC is the Federal Government's focal point for crisis response and investigation.

The NIPC is built on a foundation of partnership. When fully staffed, the NIPC will include representatives from the Federal Government (including the FBI, Department of Defense, the Intelligence Community, and others), from the owners and operators of critical infrastructures (to provide expertise and to facilitate coordination in the event of a crisis), and from state and local law enforcement (to build liaison relationships with emergency first responders). The NIPC also will establish electronic connectivity to relevant organizations in government and industry that have or require information about infrastructure threats and vulnerabilities.

The NIPC's success depends on information sharing. We are developing two-way channels of communication to facilitate information flow regarding threats, vulnerabilities, and incidents between government and industry. The Federal Government has access to

intelligence and law enforcement information that is unavailable to private organizations. Simultaneously, the NIPC wants to learn about the threats and vulnerabilities experienced by these organizations. Sharing this important information will help us to define the threat environment with greater accuracy, thereby enabling us to prevent or disrupt potential attacks.

One current initiative is "InfraGard," a pilot project sponsored by the FBI's Cleveland Field Office to foster information sharing among private industry, the FBI, and other government agencies. A secure, Internet-based system, InfraGard has an alert network that members can use to report computer intrusions to the FBI. Reports are sent by encrypted electronic mail (e-mail) in two forms: a detailed description (which the FBI uses for analysis and, if required, investigative purposes) and a sanitized, victim-produced version (for distribution to other InfraGard members). Approximately 56 organizations are now involved in the InfraGard project, and we are exploring options for expanding it into a national system.

Protecting our critical infrastructures in the Information Age will require creative solutions and new ways of thinking. Establishing the NIPC and developing a productive partnership between government and industry are important steps in this direction. Much work remains to be done, but we look forward to working with our partners as we confront the challenges ahead.

Kenneth Geide is Chief of the FBI's Computer Investigations and Operations Section (CIOS), National Infrastructure Protection Center (NIPC). Mr. Geide initiated the FBI's Economic Counterintelligence program and was instrumental in drafting and achieving the passage of the Economic Espionage Act of 1996. He received his Bachelor's Degree from the University of San Francisco and his Master's Degree from New York University.



nel, but the military in general. They used personal computers at home, used no privileged information - not even a DoD phone book - and did not use any on-line services that perform investigative searches for a fee.

In less than five minutes on the Net, Ashley, starting with only the general's name, was able to extract his complete address, unlisted phone number, and using a map search engine, build a map and driving directions to his house.

Using the same techniques and Internet search engines, they visited various military and military-related web sites to see how much and the types of data they could gather. What they discovered was too much about too much, and seemingly too little concern about the free flow of information versus what the public needs to know.

For example, one web site for a European-based installation provided more than enough information for a potential adversary to learn about its mission and to possibly craft an attack. Indeed, the web site contained an aerial photograph of the buildings in which the communication capabilities and equipment were housed. By pointing and clicking on any of the buildings, a web surfer would learn the name of the communications system housed in the building and its purpose.

"DATAMINING" MADE EASY

Taking their quest for easily accessible information one step further, the Joint Staff decided to see how much information could be collected just by typing a military system acronym into an Internet search engine. While not everyone would be familiar with defense-related acronyms, many of them are now batted around the airwaves on talk shows and on the Internet in military-related chat rooms. They soon discovered how easy it was to obtain information on almost any topic, with one web site hyper-linking them to another on the same topic.

What the Joint Staff was doing when they collected their information is commonly called "data mining" — surfing the Net to collect bits of information on individuals, specific topics or organizations, and then trying to piece together a complete picture. Individuals do it, organizations do it and some companies do it for profit.

While the information they discovered presented legitimate concerns, it wasn't all negative. The Army's Ft. Belvoir, Va., home page was cited as one example of a web site which served the needs of both the military and the public. It had the sort of information families or interested members of the public need and should get.

So what does all this mean? Is DoD creating individual and institutional security problems? In the rush to make information available to the internal audience, is too much being made available to the public and those who might want to inflict harm?

The Joint Staff doesn't pretend to have all the answers to these questions, but is encouraging users to think about these issues whenever they put information on

the Internet; and they believe that, in some cases, DoD is its own worst enemy.

Need To Know vs Right To Know











Michael J. White, DoD's assistant director for security countermeasures, agrees with the Joint Staff analysis. Moreover, as a security expert, he is concerned DoD does indeed exceed what needs to be on the Internet.

"For fear of not telling our story well enough, we have told too much," he said. "Personally, I think there's too much out there...and you need to stop and ask the question: Does this next paragraph really need to be there, or can I extract enough or abstract enough so that the intent is there without the specificity? And that is hard to do because we are pressed every day. So sometimes expediency gets ahead of pausing for a minute and thinking through the process: Does the data really need to be there? Is it going to hurt me tomorrow morning?"

DoD's policy on releasing information to the public, as spelled out by Defense Secretary William Cohen in April 1997, requires DoD "to make available timely and accurate information so that the public, Congress and the news media may assess and understand the facts about national security and defense strategy." The same statement requires that "information be withheld only when disclosure would adversely affect national security or threaten the men and women of the Armed Forces."

"On the one hand," Ashley said, "we have fast, cheap and easy global communication and coordination. On the other hand, we find ourselves protecting official information and essential elements of information against point-and-click aggregation. Clearly, this balancing act is a function of risk management. Full openness and full protection are equally bad answers. We have a serious education, training and awareness issue that needs to be addressed."

10 Things NOT to put on a DoD WEBSITE

-  Classified, for official use only or unclassified sensitive information
-  DoD contractor proprietary information
-  Privacy Act information
-  Sensitive mission data, such as unit capabilities or performance
-  System capabilities, vulnerabilities, concept of operations, architectures
-  Social Security number
-  Home address
-  Date of birth
-  Detailed family members information or pictures
-  Itineraries

The Joint Staff repeatedly returns to the issue of "point-and-click aggregation" as a problem that is often overlooked when military personnel and organizations place data on the Internet. What they're referring to is the ability to collect bits of information from several different web sites to compile a more complete picture of an individual, issue or organization with very little effort.

"The biggest mistake people make is they don't understand how easy it is to aggregate information," Walsh said.

The lesson from this is that even though what is posted on the Net is perfectly innocent in and by itself, when combined with other existing information, a larger and more complete picture might be put together that was neither intended nor desired.

A more obvious problem, yet still one not always considered when posting information on the Internet, is that the "www" in web site addresses stands for "world wide" web. Information posted may be intended only for an internal audience - perhaps even a very small and very specific group of people. But on the Net, it's available to the world.

This, security experts agree, is an enormous change from the time when foreign intelligence gathering was extremely labor intensive and could only be done effectively on U.S. soil.

"If I'm a bad guy, I can sit back in the security of my homeland and spend years looking for a vulnerability before I decide to take a risk and commit resources," Ashley said. "I'm at absolutely no risk by doing that. I can pick out the most lucrative targets before hand, and may even just bookmark those targets for future use. We won't know something has been compromised until it's too late."

White agrees with the Joint Staff's concern. "You can sit in Germany and have access to the United States just as easily as you can in Australia or the People's Republic of China or Chile," White said. "It doesn't matter where you are. You

can go back and forth and in between and lose your identity on the net instantaneously. Those who seek to use the system feel comfortable they won't be discovered."

FOUO Means FOUO

In addition to these issues, security experts see another recurring and disturbing problem. In the rush to take advantage of the Net's timeliness and distribution capabilities, military personnel are forgetting about or ignoring the For Official Use Only policies which previously made the information more difficult to obtain. Yet anyone using the Internet doesn't have to venture far into the array of military web sites to come across one which

**"We have a serious
education, training
and awareness issue
that needs to be
addressed."**

states: "For Official Use Only."

If the information is For Official Use Only, security experts said web site developers, managers and commanders must ask themselves whether the information should be there in the first place.

While officials are most concerned about the information being placed on military web sites, they had similar warnings about individual or family web sites. The Joint Staff recommends the same precautions should apply at home, especially as personnel move into high-ranking, key leadership positions.

IT'S A COMMANDER'S ISSUE

At a time when the flow of information is beyond anyone's capability to either digest it or control its direction, it's not likely the problems brought forward recently by the Joint Staff will be solved any time soon. The first step, security experts said, is awareness the problems exist. Commanders have to

understand not just the information capabilities of the world wide web, but the information vulnerabilities as well.

The second step, Walsh pointed out, is for commanders to become actively involved in the issue of what's being put on the Internet. Current DoD policies require that local commander, public affairs and security reviews prior to release of data on web pages. But the flow of information is so great, these reviews may not be occurring and few are looking at the aggregation problem.

"I think it would be very appropriate for a public affairs officer to be the commander's lead representative," Walsh said. "But it's a commander's issue and it should go down command lines. This is certainly an operational security issue. Just like operational security is everybody's business, this ultimately is everyone's responsibility."

White concurred and recommends installations create "security-integrated product teams" which would be tasked to develop and implement guidelines for creating and monitoring web sites on the installation.

"I think having a group come together before the (web site development) process begins will remove an awful lot of pain in the long run," White said. "We need to step back one step and think before we begin any effort, because once it's done you can't undo it. That makes it very hard in a digital environment."

Although it's not possible to retrieve what's already on the world-wide web, nor predict how it will influence future security issues, Walsh, Ashley and White believe it's not too late to make a difference. With a little more forethought and a lot more planning, it will be possible to better protect the next generation of warfighters, both on and off the battlefield, they said.

Previously released September 25, 1998 via DefenseLink, from the American Forces Information Service News Articles. Downloadable version is available at <http://websecurity.afis.osd.mil>.

Intrusion Detection System Evaluation

by Dr. Marc A. Zissman & Dr. Richard P. Lippmann, Lincoln Laboratory, MIT

The Information Systems Technology Group of MIT Lincoln Laboratory, under Defense Advanced Research Projects Agency Information Technology Office (DARPA/ITO) and Air Force Research Laboratory (AFRL/SNHS) sponsorship, is collecting and distributing the first standard corpus for evaluating computer network intrusion detection systems. Along with AFRL/SNHS, we are also coordinating the first formal, repeatable, and statistically significant evaluation of intrusion detection systems. This evaluation will measure probability of detection and probability of false alarm for each system under test.

This evaluation will contribute significantly to the intrusion detection research field by providing direction for research efforts by objectively calibrating current technology. The evaluation is designed to be simple, to focus on core technology issues, and to encourage wide participation. We have tried to eliminate security and privacy concerns, and we are providing data types that are used commonly by the majority of intrusion detection systems.

Technical Objective

The evaluation objectively measures intrusion detection systems' ability to detect attacks on computer systems and networks. The evaluation focuses on UNIX workstations, and the goal is to determine whether any of the following attack events occurred or were attempted during a given network session:

- Denial of service;
- Unauthorized access from a remote machine;
- Unauthorized access to local superuser privileges by a local unprivileged user;
- Surveillance and probing; and
- Anomalous user behavior.

Network sessions used for scoring the evaluation are complete TCP/IP connections, which correspond to interactions using many

services including telnet, HTTP, SMTP, FTP, finger, rlogin, and others. Because the evaluation is based on the context of normal computer use on a military base, the frequency and character of the network sessions generated for each of these services reflect their actual usage at Air Force bases worldwide. The

mal background traffic sessions, the current evaluation will allow us to measure both detection and false alarm rates simultaneously.

Data and Guidelines

Before the evaluation begins, seven weeks of training data will be made available to the participants.

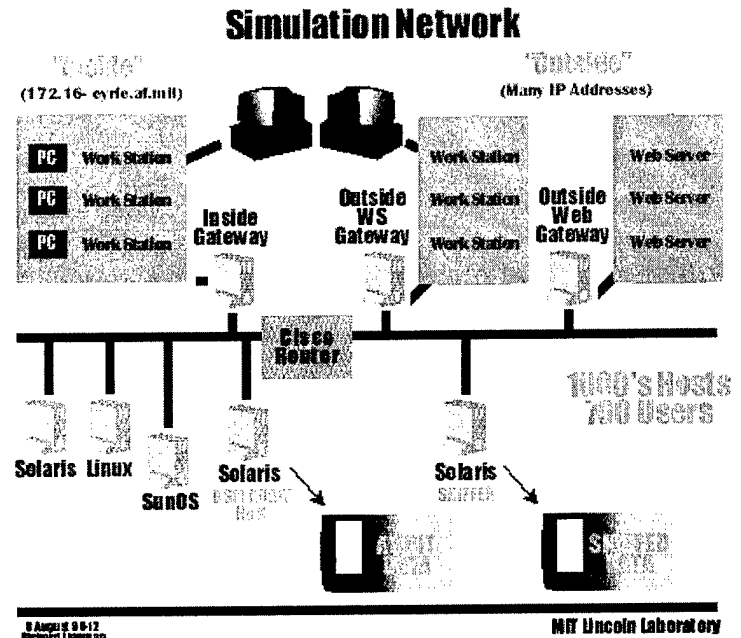


Figure 1. The Lincoln simulation network is used to generate traffic for the DARPA 1998 evaluation. The network has an "inside," which represents a military base, and an "outside," which represents the internet. Though the network contains only 10 computers, it is capable of producing traffic from thousands of simulated computers and hundreds of simulated users.

evaluation is designed to foster research progress, with the following four goals:

1. Explore promising new ideas in intrusion detection;
2. Develop advanced technology incorporating these ideas;
3. Measure the performance of this technology; and
4. Compare the performance of various newly developed and existing systems in a systematic, careful way.

Previous evaluations of intrusion detection systems have tended to focus exclusively on the probability of detection, without regard to probability of false alarm. By embedding attack sessions within nor-

These data will be used to configure intrusion detection systems and train free parameters. Generally, the types of training data provided will be those that are used by most current commercial and research intrusion detection systems, e.g., network packet traffic, host audit files, and file system dumps. These data will be labeled individually as either normal or attack/anomalous. Later, a set of test data will be made available. Evaluation participants will run their systems blindly over the test data and will submit the system hypotheses for scoring.

Both the training and the testing data will be extracted from a simu-

lation network of about a dozen workstations (see Figure 1 on opposite page). With kernel modifications made available by AFRL/SNHS and other custom software, these few workstations can emulate thousands of workstations with hundreds of users. Both normal use and attack sessions will be present. Distributions of normal session types and normal session content will be similar to that on military bases. Attack sessions will contain old, recent, and new attacks. Most network sessions are run automatically, while a small number of sessions are generated by live users. Seven weeks of network traffic are available for training, and another two weeks will be used for evaluation. In all, the evaluation corpus will contain millions of network connections.

There are two parts to the intrusion detection evaluation. The first part is an off-line evaluation. Network traffic and audit logs collected on a simulation network will serve as input to intrusion detection systems under test. These systems will process data in batch mode, trying to find the attack sessions in the midst of normal activity. The second part of the evaluation is conducted in real-time. Systems will be delivered to

AFRL/SNHS and inserted into their network testbed. Again, the job of the detection system is to find the attack sessions in the midst of normal background activity. Some systems may be tested in off-line mode, some in real-time mode, and some in both modes.

Schedule

Data for this first evaluation will be made available during the fall of 1998. The evaluation itself will occur in October and November. A follow-up meeting for evaluation participants and other interested parties will be held in December to discuss research findings. All R&D sites that find the task and the evaluation of interest are invited to participate.

For more information or to request copies of the training corpus, contact:

Dr. Marc A. Zissman or
Dr. Richard P. Lippmann
Lincoln Laboratory
Massachusetts Institute of Technology, Information Systems
Technology Group
244 Wood Street
Lexington, MA 02420-9185
Voice: 781.981.7625
Fax: 781.981.0186
Email: INTRUSION@SST.LL.MIT.EDU
HTTP://WWW.LL.MIT.EDU/IST/

For specific information on the real-time evaluation, contact:

Terrence (Terry) G. Champion
Air Force Research Laboratory
Electromagnetics Technology Division, INFOSEC Technology Office,
Building 1124
Hanscom AFB, MA 01731-5000
Voice: 781.377.2068
Fax: 781.377.2563
Email: TGC@SAPPHO.RL.AF.MIL

Marc A. Zissman received the S.B. degree in computer science from MIT in 1985, and the S.B., S.M., and Ph.D. degrees in electrical engineering all from MIT in 1986, 1988, and 1990, respectively. He is presently assistant leader of the Information Systems Technology Group at MIT Lincoln Laboratory, where his research focuses on digital speech processing and computer network security. He may be reached at MAZ@SST.LL.MIT.EDU.

Richard P. Lippmann received a B.S. in electrical engineering from the Polytechnic Institute of Brooklyn in 1970 and a Ph.D. in electrical engineering from the Massachusetts Institute of Technology in 1978. He is presently a senior staff member in the Information Systems Technology Group at MIT Lincoln Laboratory, where his research focuses on speech recognition and the application of neural networks and statistics to problems in computer intrusion detection. He may be reached at RPL@SST.LL.MIT.EDU.

Defense Wide Information Assurance

continued from page 2

them, these two teams accomplish the overall mission, tasks, and functions of the DIAP and are staffed by a combination of Service, Joint Staff, OSD, and Defense Agency personnel. The FEIT consists of eight functional areas, including Readiness Assessment, Human Resources Development, Operational Policy and Doctrine Implementation, Security Management, Operational Monitoring, Architectural Standards and System Transformation, Acquisition and Product Development, and Research and Technology. These team members are the DIAP's principal evaluators for each functional area and will continuously evaluate Component IA programs to ensure the Defense-wide application of these functions

is consistent, integrated, efficient, and programatically supported. The PDIT will provide for the oversight, coordination, and integration of the Department's IA resource programs. The sum total of these activities will ensure the Department's IA operational capabilities to protect, detect, and respond are appropriately met.

The transformation of IA from a largely technical issue to an operational imperative is critical to success of the Department's IA strategy. The DIAP constitutes a significant management, organizational, and cultural change within the Department. It will ensure that the Department's IA programs extend beyond traditional Service and Agency perspectives to meet the

growing challenges of a dynamic, global information environment. Through this process, the Department will be able to leverage information and information technology to enhance the efficiency of its business activities and the impact of its military operations.

CAPT Burton received her M.S. in National Security Strategy from the National War College and her M.A. in Management Information Systems from George Washington University. She is currently assigned as the Staff Director, Defense Wide Information Assurance Program (DIAP), in the Information Assurance Directorate of the Office of the Assistant Secretary of Defense for Command, Control, Communication and Intelligence.

The IATAC Information Assurance Tools Database hosts information on intrusion detection, vulnerability analysis, firewalls and antivirus applications. A brief summary of FIREWALL TOOLS is provided on these two pages. For more information, see the IATAC Product Order Form on page 15.

FIREWALLS

TITLE	COMPANY	KEYWORDS	URL
AltaVista Firewall 98	Digital Internet Solutions	Firewall, Application-Level Gateway, VPN	http://www.altavista.software.digital.com
AS/400	IBM, Inc.	Firewall, Application Gateway, Packet Filtering	http://www.ibm.com
Border Manager	Novell, Inc.	Firewall, Packet Filtering, Circuit-Level Gateways, Application-Level Gateways (Proxies), NAT, VPN	http://www.novell.com
BorderWare Firewall Server	BorderWare Technologies, Inc.	Firewall; Tri-Level: Packet Filtering, Circuit-Level Gateways, and Application Proxies; NAT, VPN	http://www.borderware.com
Brimstone/Freestone	SOS Corporation	Firewall, Hybrid	http://www.soscorp.com
Checkpoint Firewall-1	Check Point	Firewall, Stateful Inspection, Proxies, NAT, VPN	http://www.checkpoint.com
clPro-FW	Radguard	Firewall, Multi-Layer Probing (MLP), NAT, VPN	http://www.radguard.com
ConSeal PC Firewall	Signal 9 Solutions	Firewall, Packet Filtering, NAT, VPN	http://www.signal9.com
CyberGuard for NT	CyberGuard Corporation	Firewall, Hybrid, NAT	http://www.cyberguard.com
CyberGuard for UnixWare	CyberGuard Corporation	Firewall, Hybrid, NAT	http://www.cyberguard.com
Elron Firewall	Elron Software, Inc.	Firewall, Stateful Inspection, NAT, VPN	http://www.elronsoftware.com
eNetwork for AIX/ Windows NT	IBM, Inc.	Firewall, Hybrid, NAT, VPN	http://www.ibm.com
Firebox 100/ Firebox II	WatchGuard Technologies, Inc.	Firewall, Stateful Packet Filtering, Transparent Proxies, NAT, VPN	http://www.watchguard.com
Firewall for Windows NT	Secure Computing	Firewall, Application Gateway (Proxies)	http://www.elronsoftware.com
Gauntlet	Trusted Information Systems	Firewall, Application Gateway, VPN	http://www.tis.com
GemGuard	Gemini Computers	Firewall, Trusted Packet Filtering, VPN	http://www.geminisecure.com
GNAT Box	Global Technology	Firewall, Stateful Packet Inspection, Application Techniques, NAT	http://www.gnatbox.com
Guardian	NetGuard, Ltd.	Firewall, Stateful Inspection, NAT, VPN	http://www.ntguard.com
GuardIt	Computer Associates	Firewall, Hybrid, NAT	http://www.cai.com
He@tSeekerPro	Fortress Technologies	Firewall, Packet Filtering	http://www.fortresstech.com
ICE.BLOCK	J. River, Inc.	Firewall, Packet Filtering	http://www.jriver.com
Interceptor	Technologic, Inc.	Firewall, Application Proxies, VPN	http://www.tlogic.com

FIREWALLS

TITLE	COMPANY	KEYWORDS	URL
InterLock Service	WorldCom Advanced Networks	Firewall, Application-Level Proxy	http://www.ans.net
IOS Firewall Feature Set	Cisco Systems	Firewall, Packet Filtering, NAT, VPN	http://www.cisco.com
Lucent Managed Firewall	Lucent Technologies, Inc.	Firewall, Packet Filtering	http://www.lucent.com
LuciGate	Lucidata	Firewall, Packet Filtering, NAT	http://www.lucidata.com
NetGate	Small Works, Inc.	Firewall, Packet Filtering and Routing Package, VPN	http://www.smallworks.com
NetScreen-100/ NetScreen-10	NetScreen Technologies	Firewall, Dynamic Filter, NAT	http://www.netscreen.com
Norman Firewall	Norman Data Defense	Firewall, Dual-homed Gateway, Application Proxies, NAT	http://www.norman.com
PIX	Cisco Systems	Firewall, Hybrid, NAT	http://www.cisco.com
PORTUS-ES	Livermore Software Laboratories	Firewall, Proxies, NAT, VPN	http://www.lsl.com
PrivateWire	Cylink Corporation	Firewall, Dynamic Packet Filtering, VPN	http://www.cylink.com
PyroWall	Radguard	Firewall, Multi-Layer Probing (MLP), NAT, VPN	http://www.radguard.com
Raptor for NT	Axent Technologies	Firewall, Hybrid (Application-level proxies, Packet Filtering), NAT, VPN	http://www.axent.com
Raptor for Solaris	Axent Technologies	Firewall, Hybrid (Application-level proxies, Packet Filtering), NAT, VPN	http://www.axent.com
Secure Access	Ascend	Firewall, Hybrid, VPN	http://www.ascend.com
SecurIT Firewall for Solaris	Milkyway Networks	Firewall, Application and Circuit Level Gateway, Proxy Servers	http://www.milkyway.com
SecurIT Firewall for Windows NT	Milkyway Networks	Firewall, Application and Circuit Level Gateway, Proxy Servers	http://www.milkyway.com
SecureWare NetWall	Bull HN Information Systems	Firewall, Hybrid, NAT, VPN	http://www.bull.com
Sidewinder	Secure Computing	Firewall, Application Gateway (Proxies), VPN	http://www.securecomputing.com
SmartWall	V-ONE Corporation	Firewall, Packet Filtering, Proxies, NAT, VPN	http://www.v-one.com
Solstice Firewall-1	Sun Microsystems	Firewall, Stateful Inspection, VPN	http://www.sun.com/security
SonicWALL	Sonic Systems, Inc.	Firewall, Stateful Inspection, NAT	http://www.sonicsys.com
StoneBeat	Stonesoft Corporation	Firewall, High Availability	http://www.stonebeat.com
Telaxian Shield Firewall Server	Network Engineering	Firewall, Hybrid, NAT, VPN	http://www.fireants.com
WinGate	Deerfield Communications, Inc.	Firewall, Proxy server	http://www.deerfield.net

ia tools

Summary

Detecting Intrusions Cooperatively Across Multiple Domains

by Donald L. Tobin, Jr.
University of Idaho

In the national defense arena, most analysts pay little attention to the isolated cases of computer intrusions reported almost weekly in the news. If analysts became aware of a pattern of attacks directed at a variety of networks and domains, however, this information might well warrant heightened attention. Our research efforts at the University of Idaho are directed in part at developing a prototype to supply multiple-domain information.

Commercial intrusion detection systems protect only a single network or a collection of networks in a single domain, such as pentagon.mil or lajes.af.mil. These limitations make it difficult even to detect a sweep or scan attack against multiple government and military installations in a single geographic area, especially if they represent different departments like the Department of Defense and the Department of Energy,

or different services, such as the Army, Air Force, and Navy. A seemingly insignificant intrusion at one location would acquire much greater importance if collaboration among the installations revealed a coordinated set of attacks. Therefore, some form of data sharing is needed to detect systemic attacks against the nation's critical information infrastructure that involve multiple hosts and domains.

To help address these concerns, we have developed a prototype called HMMR (Hierarchical Management of Misuse Reports) or Hummer. The prototype and its source code are available at <http://www.cs.uidaho.edu/~hummer>. When HMMR is fully deployed, every host has a Hummer running on it, and all the hosts in a domain are probably, but not necessarily, arranged in some hi-

erarchical fashion. Each domain has a top-level manager, and those managers may agree to form peer groups with top-level managers from other domains. Peer groups can also be formed among cooperating systems at other levels. In the hierarchical model, manager and subordinate systems do not have to be in the same domain.

The Hummers can collect data such as log files, usage reports, commercial tools, and freeware security tools and scanners from several locations on their host machine and put the acquired data into a common format. However, these capabilities require that additional coding to extract data from the source and then reformat it properly for the Hummer to use and distribute, depending

to a situation with only a few clicks of the mouse button. Once a top-level manager has created a particular configuration, he can push the configuration, including the filters to be used, out to all the other Hummers under him in the hierarchy in a few minutes.

The following scenario illustrates the Hummer's use. A Department of Energy (DOE) research laboratory located near an Army installation, an Air Force installation, and a major government contractor has formed a peer group with the other facilities using HMMR so the organizations may share security-related information. Normally, the data collection, logging, and auditing tools run in the background at the DOE lab; to avoid negative impact on the user community, only a small subset of Hummer tools are routinely turned on. One day, however, an alert system administrator sees Hummer-generated information

being passed to her system from the Army installation and the government contractor, in turn, indicating they have been subjected to port scans. Expecting her network to be the next likely target, the system administrator turns on additional logging immediately, confident that with a few keystrokes, the more information she has, the better her chances of inhibiting the intruder.

Hummer represents only one of many areas in our ongoing research. The most important area, we believe, is developing a formal trust, integrity, and cooperation (TIC) model among hosts across multiple domains. We recognize that data, or even data requests, from a peer may be unreliable, inaccurate, or deliberately falsified, yet there remains a need to use available global information to ac-



on the filters created by that host's system administrator or high-level managers/administrators. The reformatted information is distributed, either through the hierarchy or to all the other peers in the peer group. The filter is simply a screen that determines which security-relevant information is to be shared with other hosts and networks. The filters can be generated quickly through one of the user interfaces.

Each Hummer has a World Wide Web-based interface for relatively easy configuration and management operations. The Audit Tool Manager lets the user pick which tools to use at any time. It also offers preconfigured suites of tools for "Possible Intrusion" and "Ongoing Intrusion" alert levels. These resources allow the operator to turn on all policy-defined tools and respond

continued on page 13

Secure Your Distributed Network: What Will It Take?

by Robert Duchatellier
Lucent Technologies

Today's enterprises rely on the World Wide Web to deliver timely information to a broad base of users, branch offices, partners, and customers. As more information, content, and applications become readily available via the Internet and via intranets and extranets, you must look closely at the security requirements of your organization's servers, systems, and networks and ensure that you protect these critical assets.

Intranets, extranets, and the Internet are changing our world. They distribute information and services to people, no matter where they are. But most network security systems were never designed for distributed environments. As a result, they cannot deliver the scalability and management control needed to support growth and still remain secure.

Web site databases and other application systems are compromised almost every day, sometimes inadvertently, sometimes with malicious intent, and sometimes for the so-called fun of "breaking in." No system is absolutely impervious to attack, from both internal and external individuals and groups, but you can take steps to protect your systems, and

you can implement policies and procedures to reduce significantly the threat of unauthorized access. One approach to achieving these goals is use of the Lucent Managed Firewall, now available in version 3.0.

Originally engineered by Bell Labs to protect Lucent Technologies' networks, the Firewall is designed to be intrinsically secure. It physically separates the security and management functions to improve each function's security and performance.

Lucent Technologies

The Lucent network security appliance, called "the Brick," is a bridge-level device that runs Inferno™ operating system software, a compact, real-time operating system. The firewall code is embedded in the Inferno operating system kernel. The Brick eliminates common points of vulnerability, including user logins, files, hard drive, and monitor. The resulting firewall is hard to break and easy to maintain.

The Security Management Server software handles administrative functions. Available for Windows NT® and Sun Solaris® op-

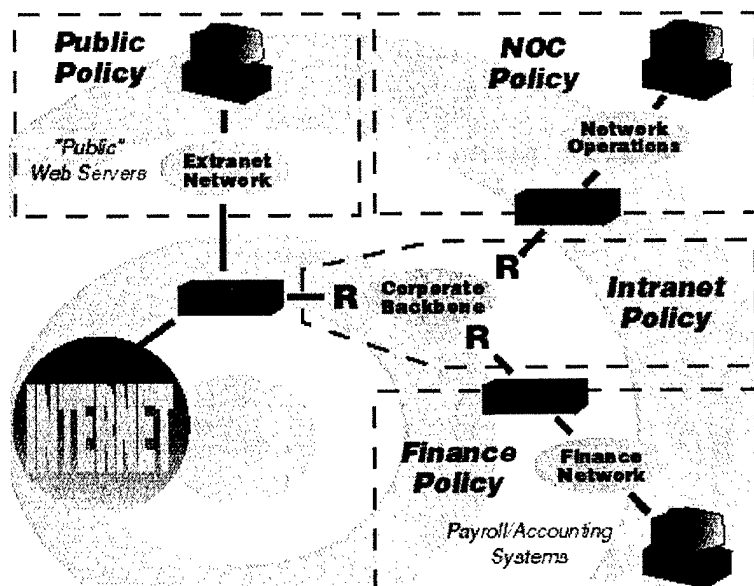
erating systems, the Security Management Server features an easy to use graphical user interface (GUI). As a result, network administrators do not have to be versed in operating systems or network configuration to manage the system.

The Brick uses native encryption and authentication features to communicate securely with the Security Management Server. The administrator works with the Security Management Server using encrypted sessions via indus-

try-standard Secure Sockets Layer (SSL) and Design Engineering Services (DES) encrypted links, all of which are built in. Included with the Lucent Managed Firewalls is a free X.509 digital certificate from VeriSign.

Additionally, the Lucent Managed Firewall is extremely scalable and easy to deploy. Most firewalls establish security rules geographically or physically. Instead, Lucent uses security zones to establish rules logically. One Brick can support multiple security policies or "zones," and each security zone can be set up to have its own distinct set of rules, with report logs and alarms customized for that zone. Multiple zones can be managed centrally from one Security Management Server. This approach makes it easy for you to enforce multiple security policies across multiple Bricks, regardless of where your firewalls are located.

The Lucent Managed Firewall can easily scale up to meet your needs, no matter how large they become. As the network grows, you simply add Bricks to the Security Management System. Because the firewall appliance is implemented as a bridge, not a router, you can add new firewall appli-



continued on page 12

IA Scientific & Technical Information

by Robert P. Thompson
Director, IATAC

Collection of scientific and technical information (STI) is essential to Information Analysis Center (IAC) operations. The Information Assurance Technology Analysis Center (IATAC) collection of Information Assurance (IA) STI focuses on technologies that support the design, development, testing, evaluation, operations, and maintenance of Department of Defense (DoD) military systems and infrastructure. STI products and services serve to advance the knowledge base and productivity of the DoD research, development, test, and evaluation (RDT&E) community.

IATAC taps many sources to collect IA STI. It relies on direct interface with vendors supporting the IA community as a primary source of information. Nondisclosure agreements with corporations yield information on emerging research and development (R&D). Release of STI obtained through non-disclosure is tightly controlled as delineated in the agreement. Technical symposia and conferences also provide information, and seeks conference proceedings and technical papers often become part of the STI Collection. IATAC also interfaces with DoD and other Federal Government agencies also facilitate receipt of new scientific and technical information.

Technical Area Tasks also produce's STI and helps to build the IA collection. Finally, open source gathering techniques augment collection activities. The IATAC collection offers materials on a number of IA STI topics, including those listed below.

Information in the IA STI collection is available to registered Defense Technical Information Center (DTIC) users. Secondary distribu-

tion instructions must be strictly followed to ensure compliance with copyright restrictions. To become a registered DTIC user, applicants must complete DD Form 1540 available from <http://web1.whs.osd.mil/icdhome/DDEFORMS.HTM>.

For more information on the IA STI Collection, contact IATAC at 703.902.3177 or via email at iatac@dtic.mil.

STI Topics

- | | |
|--|----------------------------|
| ☛ Command, Control, Communications, Computers & Intelligence (C4I) | ☛ Information Warfare |
| ☛ Computer Network Attacks (CNA) | ☛ Infrastructure Assurance |
| ☛ Encryption | ☛ Intrusion Detection |
| ☛ Firewalls | ☛ Malicious Code Detection |
| ☛ Hackers | ☛ Red Teaming |
| ☛ Information Assurance | ☛ Vulnerability Analysis |
| ☛ Information Operations | ☛ Virus/Anti-Virus |
| | ☛ Year 2000 (Y2K) |

Secure Your Network

continued from page 11

ances at any time without reconfiguring the router network. With the release of the Lucent Managed Firewall v3.0, you can also manage software downloads remotely, saving time and maintenance expense.

The Lucent Managed Firewall can operate in a gateway perimeter setting to protect an enterprise network from the Internet or from partner extranet networks. It can separate public Web servers from sensitive intranet servers. It can also separate different intranet segments. Its scalability and flexibility can handle virtually any type of application, as well as any

size and type of infrastructure.

Your network applications and systems are only as secure as the weakest point of entry. To secure your network, you must design the system to provide distributed security, centralized management and scalability. You must also adhere to strict policies and train users effectively. Implementing these steps and deploying advanced firewall technology will provide a secure system to support a broad range of applications, while minimizing the threat from unwelcome guests. These components build the strong foundation required to ensure maximum se-

curity while they also deliver the flexibility needed to grow your enterprise.

For more information, contact Lucent Technologies at 888.552.2544 or on-line at <http://www.lucent.com/security>.

Robert Duchatellier received an M.S. in Industrial and Applied Mathematics from Brooklyn Polytechnics Institute and an M.S. in Technology Management from Stevens Institute of Technology. He is currently Lucent Technologies' Lucent Managed Firewall Sales Channel Manager for the U.S. Government, Department of Defense, and Federal Agencies.

**NOV
1-5**

25th Annual Computer Security Conference & Exhibition
Sponsored by Computer Security Institute (CSI)
Chicago, IL
call 415.905.2378
www.gocsi.com

**NOV
2-5**

The Defense Technical Information Center (DTIC) Annual Users Meeting and Training Conference
DoubleTree Hotel
National Airport, Arlington, VA
call Ms. Julia Foscue
703.767.8236
jfoscue@dtic.mil
<http://www.dtic.mil>

**NOV
4-5**

13th Annual Mid-Atlantic Intelligence Symposium
Sponsored by AFCEA Central Maryland Chapter
Johns Hopkins Applied Physical Lab (APL), Laurel, MD
call Dawn Metzger 410.684.6580

**JAN
19-21**

AFCEA West '99
Sponsored by AFCEA and the U.S. Naval Institute
San Diego, CA
call the AFCEA Programs Office
703.631.6125 / 6126

**MAR
2-4**

Southeast C4I Conference and Exposition
Sponsored by the AFCEA Tampa — St. Petersburg Chapter
Tampa, FL
call J. Spargo & Associates
703.631.6200

DTIC's Annual Users Meeting & Training Conference

This year DTIC is hosting its 25th Annual Users Meeting and Training Conference. The conference will be held at the DoubleTree Hotel National Airport, 300 Army Navy Drive, Arlington, VA, from 2-5 November 1998. The agenda is packed full of exciting and relevant topics, as well as an exhibit room overflowing with vendors from every aspect of Information Technology (IT).

"Maintaining the Information Edge" is the theme for the conference, and the sessions are geared to this topic. DTIC '98 will address the information sources and changing technologies that impact those who are involved in Defense Research and Acquisition. We are particularly pleased to announce this year's keynote speakers: Lieutenant General David J. Kelley, Director, Defense Information Systems Agency; Mr. Carol Cini, Associate Director, U.S. Government Printing Office; and Mr. Richard Luce, Director, Los Alamos Research Library. Mr. Louis Purnell, the luncheon speaker, will be relating his exploits during World War II as a Tuskegee Airman.

The Conference offers four days of varied training sessions that enable DTIC users to collaborate on the latest IT topics. Presentations will address the most current issues effecting the research, development, and acquisition communities. Not only will these speakers acquaint you with the latest policy and operational developments, but they will also provide you with practical details on valuable and diverse domestic and foreign information resources, security issues, the World Wide Web, virtual libraries, video streaming and the storage and dissemination of electronic documents.

Maintaining the Information Edge presents exciting new challenges — DTIC '98 promises to provide the tools to expand your horizons to meet these challenges! For more information, please contact Ms. Julia Foscue, the DTIC '98 Conference Coordinator at 703.767.8236 or via e-mail: jfoscue@dtic.mil, or access the DTIC homepage at <http://www.dtic.mil>.

Detecting Intrusions

continued from page 10

curately assess the local security posture. Therefore, a formal model must include multiple levels of cooperation and trust and must provide concise definitions of cooperation and trust in this context. Other considerations to be addressed are whether the cooperation levels should be statically or dynamically assigned and how quickly or gracefully they should be adjusted in response to the most current data. The model must also take into account the various costs of cooperation, including data collection, transmission,

and sanitization and the exposure risk of the local network.

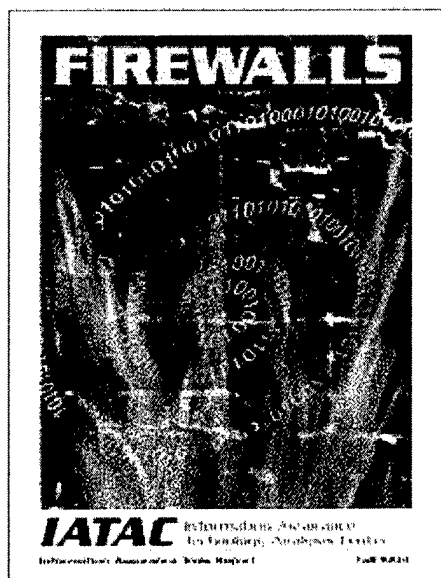
While most of the structure has been coded by undergraduates (Jamie Marconi, Jesse McConnell, Dean Polla, and Joel Marlow) so far, we hope our work on Project HMMR and our future research will encourage other researchers to explore new ideas for addressing the risks facing the critical information infrastructure. We have shown that cooperative intrusion detection can be achieved, and we believe it must be

achieved to help ensure national security in the future.

Donaki Tobin is a doctoral student at the University of Idaho and a research assistant at the Center for Secure and Dependable Software. His primary research interests are in intrusion detection, neural networks, and information warfare. He is a retired Air Force officer and has worked with a variety of communication, satellite, and missile warning systems. He earned his M.S. in Computer Science from Boston University and his B.S. in Mathematics from the University of Texas.

IA Tools Report: FIREWALLS

New Products



The Information Assurance (IA) Tools Report on Firewall tools is now available to registered DTIC users. This report provides an index of firewall products contained in the IA Tools database. It summarizes pertinent information, providing users with a brief description of available tools and contact information. As a living document, this report will be updated periodically as additional information is entered into the database.

Currently the IA tools database contains 46 firewall tools that are available in the commercial marketplace or through GSA contracts. The

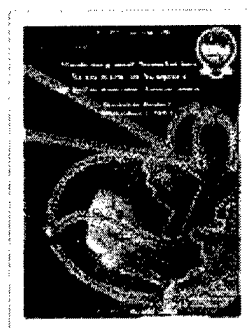
firewall products provide a range of solutions to meet various firewall requirements. These solutions can provide protection of internal networks and provide secure Internet and remote access connections. The database was built by gathering open-source data, analyzing that data, coordinating with the respective firewall developer, and then formatting the data into the final report. The information includes a basic description, security services and mechanisms, availability, contact, and reseller/ distributors for each firewall product included. For instructions on obtaining a copy of this report, refer to the IATAC Product Order Form.



**IA Tools Reports —
Vulnerability Analysis &
Intrusion Detection**

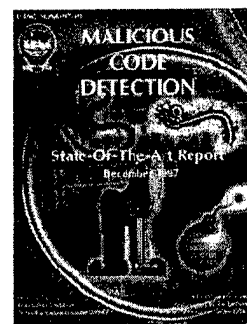
This IA Tools reports summarize pertinent information, providing users with a brief description of available tools and contact information. As living documents, these reports will be updated periodically as additional information is entered into the databases.

Currently the Vulnerability Analysis IA Tools database contains descriptions of 35 tools that can be used to support vulnerability and risk assessment. Research for the Intrusion Detection IA Tools report identified 43 intrusion detection tools currently employed and available.



**Modeling & Simulation
Technical Report**

This report describes the models, simulations and tools being used or developed by selected organizations that are chartered with the IA mission. The definitions prescribed by DMSO for model and simulation were used to determine what entities should be included in this IA models, simulations and tools report.



**Malicious Code Detection
State-Of-The-Art Report**

This SOAR addresses malicious software detection. Included is a taxonomy for malicious software to provide the audience with a better understanding of commercial malicious software. An overview of the current state-of-the-art commercial products and initiatives, as well as future trends is presented. The same is then done for current state-of-the-art in regards to DoD. Lastly, the report presents observations and assertions to support the DoD as it grapples with this problem entering the 21st century.



IATAC Product Order Form

IMPORTANT NOTE: All IATAC Products are distributed through the Defense Technical Information Center (DTIC). If you are NOT a registered DTIC user, you must do so PRIOR to ordering any IATAC products. To register with DTIC go to <http://www.dtic.mil/dtic/regprocess.html>.

Name _____

Organization _____ Ofc. Symbol _____

Address _____

Phone _____

E-mail _____

Fax _____

DoD Organization? ☐ YES ☐ NO If NO, complete LIMITED DISTRIBUTION section below.

LIMITED DISTRIBUTION

QTY.

PRICE EA.

EXTD. PRICE

In order for NON-DoD organizations to obtain LIMITED DISTRIBUTION products, a formal written request must be sent to IAC Program Office, ATTN: Sherry Davis, 8725 John Kingman Road, Suite 0944, Ft. Belvoir, VA 22060-6218

Contract No. _____

For contractors to obtain reports, request must support a program & be verified with COTR

COTR _____ Phone _____

<input type="checkbox"/> Modeling & Simulation Technical Report		No Cost	
<input type="checkbox"/> IA Tools Report — Firewalls		No Cost	
<input type="checkbox"/> IA Tools Report — Intrusion Detection		No Cost	
<input type="checkbox"/> IA Tools Report — Vulnerability Analysis		No Cost	
<input type="checkbox"/> Malicious Code Detection SOAR <input type="checkbox"/> TOP SECRET <input type="checkbox"/> SECRET		No Cost	

Security POC _____

Security Phone _____

UNLIMITED DISTRIBUTION

QTY.

PRICE EA.

EXTD. PRICE

<input type="checkbox"/> Newsletters (Limited number of back issues available)			
<input type="checkbox"/> Vol. 1, No. 1 <input type="checkbox"/> Vol. 1 No. 2 <input type="checkbox"/> Vol. 1 No. 3		No Cost	
<input type="checkbox"/> Vol. 2, No. 1 <input type="checkbox"/> Vol. 2 No. 2			

ORDER TOTAL

Please list the Government Program(s)/Project(s) that the product(s) will be used to support: _____

Once completed, Fax to IATAC at 703.902.3425

ARE sharing your

I/A newsletter

FOR ADDITIONS, DELETIONS AND CHANGES

— U.S. Distribution Only —

Copy this page, complete the form and fax to IATAC at 703.902.3425

☐ Change ☐ Add ☐ Delete

Name _____ Title _____

Company/Org. _____

Address _____

City/State _____ Zip _____

Phone _____ Fax _____

DSN _____ E-mail _____

Organization (check one):

☐ USA ☐ USN ☐ USAF ☐ USMC ☐ OSD ☐ Contractor ☐ Other _____



**Information Assurance
Technology Analysis Center**
8283 Greensboro Drive, Allen 663
McLean, VA 22102-3838